

REMARKS

I. Introduction

In response to the Office Action dated November 4, 2004, Applicants have amended Fig. 4 to include the legend "Prior Art." In this regard, Fig. 4 has not been renumbered as kindly suggested by the Examiner so as to avoid renumbering other drawings. Also, Applicants have amended claims 1, 4 and 5 so as to further clarify the claimed subject matter. Support for these amendments can be found, for example, in Figs. 1 and 3, and their corresponding sections of the specification. No new matter has been added.

Furthermore, it is noted that prior art reference, USP No. 6,490,685 B1 to Nakamura, which was submitted in the Information Disclosure Statement "IDS" filed on January 7, 2004, has not yet been indicated to have been considered by the Examiner. It is respectfully requested that the Examiner initial this reference on the PTO-1449 form that was submitted with the IDS and return the form to the Applicants so that they can confirm that the reference has been considered. Although a copy of the foregoing reference was previously submitted with the IDS, an additional copy is enclosed herewith for the Examiner's convenience.

For the reasons set forth below, Applicants respectfully submit that all pending claims are patentable over the cited prior art references.

II. The Rejection Of Claim 4 Under 35 U.S.C. § 112, Second Paragraph

Claim 4 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Specifically, the Examiner asserts that claim 4 is not "well understood since it

essentially contradicts the claims on which claim 4 depends.” In response, Applicants have amended claim 4 to recite “wherein the plural redundancy check data are stored at certain data bit positions of an address, and the plural confidential data are stored at remaining data bit positions of the same address on the ROM.” Accordingly, Applicants respectfully submit that claim 4 is now in compliance with the requirements of 35 U.S.C. § 112, second paragraph, and it is respectfully requested that this rejection of claim 4 be withdrawn in view of the foregoing amendment.

III. The Rejection Of Claims 1-5 Under 35 U.S.C. § 102

Claims 1-7 are rejected under 35 U.S.C. § 102(e) as being anticipated by USP No. 6,185,678 to Arbaugh. Applicants respectfully request reconsideration of this rejection for at least the following reasons.

Claim 1, as amended, recites in-part “... storing plural *redundancy check data* ... obtained by performing a predetermined *calculation* on *each* of the corresponding plural *confidential data*, and...a result of the calculation performed by the checker is compared to *each* of the corresponding plural *redundancy check data*....”

Specifically, in accordance with one exemplary embodiment of the present invention, the CRC 25 performs a calculation on the confidential data words read out from the ROM 10 in which the calculation carried out by the CRC 25 is substantially the same as the calculation performed to produce the confidential CRC codewords. Then, the CRC 25 outputs the result OUT of the calculation to the comparator COMP 26. In response, the comparator COMP 26 compares the output OUT of the CRC 25 to the confidential CRC codewords read out from the ROM 10. Accordingly, the present invention advantageously allows the confidential data stored

in the ROM to be error-checked without having to read out the confidential data from the integrated circuit to compromise the security level of the confidential data (see, e.g., page 3, lines 7-18 of the specification).

In contrast, Arbaugh discloses a first layer 200 which only contains the trusted software, digital signatures, public key certificates and recovery code, and does not disclose storing any data that can be interpreted as the claimed redundancy check data, let alone any data being utilized to verify the result of the alleged checker. Indeed, the stored signature of Arbaugh being relied upon by the pending rejection appears to be one of the digital signatures contained in the layer 200. As such, the alleged confidential data and the alleged redundancy check data are not *separate* and *distinct*.

Furthermore, at the portion cited in the pending rejection, Arbaugh merely defines a process in which the BIOS of the AEGIS model is modified. As expressly described at col. 8, lines 60-67, because the transition between various layers in the traditional boot process is accomplished without any attempt at verifying the integrity of each or next layer, the AEGIS model therefore uses public key cryptography and cryptographic hashes to protect its integrity by verifying the transition between each layer. This is further evidenced by the fact that the process or control at the first section 202 can only proceed to the second section 212 if the signature is valid after the cryptography verification (see, col. 9, lines 35-39). As such, at best, the cited prior art has arguably only shown how the cryptographic hash of the second section 212 is computed to verify against the stored signature without demonstrating how a redundancy check data is derived or obtained *in relation* (e.g., by performing substantially the same calculation) to the alleged confidential data. In the event it is asserted that the result of the checksum calculation corresponds to the result of the calculation performed by the alleged checker such

that it is compared with the stored signature, it is important to note that Arbaugh expressly discloses performing the standard checksum calculation...to protect against ROM failure (see, col. 9, lines 33-35). Accordingly, the checksum calculation appears *independent* from and *irrelevant* to the computation of the cryptography hash. This is also supported by the fact that Arbaugh only discloses verifying the cryptographic hash against the stored signature, but does not disclose or suggest verifying the result of the checksum calculation against the stored signature. For all of these reasons, it is respectfully submitted that Arbaugh does not disclose or suggest "... storing plural *redundancy check data* ... obtained by performing a predetermined *calculation* on *each* of the corresponding plural *confidential data*, and...a result of the calculation performed by the checker is compared to *each* of the corresponding plural *redundancy check data*..." as recited by amended claim 1.

Similarly, even assuming *arguendo* that the stored signature of Arbaugh can be construed as the claimed redundancy check data, rather than as the claimed confidential data, the alleged confidential data and the alleged redundancy check data still are not *separate* and *distinct*, because the stored signature appears to be one of the digital signatures as disclosed at col. 8, line 46. Accordingly, Arbaugh does not provide a confidential data that is different from the alleged redundancy check data. Also, in another hypothetical scenario in which the cryptographic hash is read as the claimed confidential data, it is clear that the alleged redundancy check data is not obtained by any calculation performed in relation to the cryptographic hash.

Therefore, for all of the foregoing reasons, it is respectfully submitted that Arbaugh is completely silent with regard to providing a confidential data *and* a redundancy check data, let alone disclose multiples thereof. Even assuming *arguendo* that the Examiner's interpretation is accurate, the Examiner has not provided requisite objective evidence from Arbaugh that the

alleged redundancy check data is *derived based on the checksum calculation* performed on the alleged confidential data. Indeed, it does not appear that the alleged redundancy check data and the alleged confidential have any inter-relationship therebetween, let alone to compare each redundancy check data and the alleged confidential data *correspondingly*. For these reasons, it is respectfully submitted that claim 1 is patentable over Arbaugh.

Finally, it is noted that the pending rejection references various portions of Arbaugh as allegedly disclosing the claimed features, but does not identify precisely which elements of functions (either by reference numerals or by written explanation) of Arbaugh are being read on the respective claimed features. If the Examiner maintains the pending rejection, it is respectfully requested that the Examiner identify which specific element or function of Arbaugh reads on *each* and *every* limitation recited in the pending claims rather than merely pointing Applicants to wide-ranging disclosures of Arbaugh so as afford the Applicants an opportunity to rebut and/or address the specific elements or functions identified as reading on the pending claims.

With respect to claim 5, as this claim also includes the features “storing plural redundancy check data which have been obtained by performing a predetermined calculation on each of the corresponding plural confidential data,” “...performing the same type of calculation as the predetermined calculation on each of the plural confidential data read out” and “comparing a result of the calculation...to the corresponding redundancy check data read out,” it is respectfully requested that claim 5 be allowed for reasons similar to those discussed above with respect to claim 1.

Accordingly, as anticipation under 35 U.S.C. § 102 requires that each element of the claim in issue be found, either expressly described or under principles of inherency, in a single

prior art reference, *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 USPQ 781 (Fed. Cir. 1983), and at a minimum, Arbaugh fails to disclose or suggest the foregoing claim elements, it is clear that Arbaugh does not anticipate claim 1 or 5, or any of the claims dependent thereon.

IV. All Dependent Claims Are Allowable Because The Independent Claims From Which They Depend Are Allowable

Under Federal Circuit guidelines, a dependent claim is nonobvious if the independent claim upon which it depends is allowable because all the limitations of the independent claim are contained in the dependent claims, *Hartness International Inc. v. Simplimatic Engineering Co.*, 819 F.2d at 1100, 1108 (Fed. Cir. 1987). Accordingly, as independent claims 1 and 5 are patentable for the reasons set forth above, it is respectfully submitted that all claims dependent thereon are also in condition for allowance.

V. Conclusion

Accordingly, it is urged that the application is in condition for allowance, an indication of which is respectfully solicited.

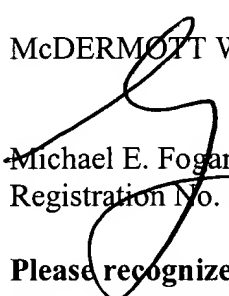
If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicants' attorney at the telephone number shown below.

Application No.: 09/867,766

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 MEF/AHC
Facsimile: 202.756.8087
Date: **March 28, 2005**

**Please recognize our Customer No. 20277
as our correspondence address.**

WDC99 1055486-1.060188.0075

Application No.: 09/867,766

IN THE DRAWINGS

Please amend Fig. 4 as indicated on the enclosed copies thereof. Fig. 4 has been amended to include the legend "Prior Art."